In the Claims:

Please amend claims 1, 5, 18, 23, and 42-43, and cancel claims 35-39, all as shown below.

1. (Currently Amended): A security system for allowing a client to access a protected resource through an application container, the security system comprising:

~~an~~ the application container, which provides services for a protected resource, wherein the application container delegates authorization decisions to a security service by passing an access request and a callback handler to the security service when the application container receives the access request for a protected resource from [[a]] the client;

context information, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client;

the security service for making a decision to permit or deny the access request, wherein a plurality of security plug-ins that implement an access decision interface are plugged into the security service, and wherein the plurality of security plug-ins use the callback handler to request the context information from the application container for the access request, and wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles ~~can be~~ is computed dynamically at runtime, and wherein depending on output from each security plug-in the security service determines entitlements for the client to use with the protected resource; and

the security service is located at a first computer, and the protected resource is located either at the first computer or at a second computer.

2. (Previously Presented): The security system of claim 1 wherein the application container of claim 1 reads an application deployment description and registers the application deployment description within the security service.

3. (Canceled)

4. (Previously Presented): The security system of claim 2 wherein the application container is a Web Application container.

5. (Currently Amended): The security system of claim 1 wherein each of the plurality of security plug-ins ~~can~~ determines a contributory decision to permit, deny, or abstain from the access request.

6. (Previously Presented): The security system of claim 5 wherein the security service further includes an access controller for transferring the access request to the plurality of security plug-ins, and for combining the contributory decisions into an overall decision by the security service to permit or deny the access request.

7. (Previously Presented): The security system of claim 5 wherein one or more of the plurality of the security plug-ins represent a business function related authorization policy.

8. – 9. (Canceled)

10. (Previously Presented): The security system of claim 5 wherein a deny or abstain by any one of the plurality of security plug-ins causes the security service to deny the access request.

11. (Previously Presented): The security system of claim 5 wherein an abstain by any one of the plurality of security plug-ins does not cause the security service to deny the access request.

12. (Previously Presented): The security system of claim 5 wherein the security service further includes security plug-ins that implement an audit interface for auditing the determinations of the plurality of access requests.

13. – 17. (Canceled)

18. (Currently Amended): A method of allowing a client to access a protected resource through an ~~Application Container~~ application container, the method comprising:

receiving at ~~an~~ the application container, which provides services to the resources it contains, an access request from the client to access the protected resource;

communicating the access request from the application container to a security service with the access request and a callback handler, wherein the application container delegates authorization decisions to the security service by passing ~~an~~ the access request and [[a]] the callback handler to the

security service when the application container receives ~~an~~ the access request for the protected resource from [[a]] the client;

making a decision at the security service to permit or deny the access request, wherein a plurality of security plug-ins that implement an access decision interface are plugged into the security service;

using the callback handler at each security plug-in to request context information from the application container for the access request, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client;

determining entitlements for the client to use with the protected resource depending on output from each security plug-in, wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein the association of the client to roles ~~can be~~ is computed dynamically at runtime; and

communicating a permitted access request to the protected resource.

19. (Previously Presented): The method of claim 18 wherein the application container of claim 18 reads an application deployment description and registers the deployment description within the security service.

20. (Canceled)

21. (Previously Presented): The method of claim 19 wherein the application container is a Web Application container.

22. (Previously Presented): The method of claim 18 further comprising:

determining at each security plug-in a contributory decision to permit, deny, or abstain from the access request.

23. (Currently Amended): The method of claim 22 further comprising:

transferring, via an access controller, the access request to the plurality of security plug-ins, and combining the contributory decisions into an overall decision by the security service to permit or deny the access request.

24. (Previously Presented): The method of claim 22 wherein one or more of the plurality of the security plug-ins represent a business function related access policy.

25. -26. (Canceled)

27. (Previously Presented): The method of claim 22 wherein a deny or abstain by any one of the plurality of security plug-ins causes the security service to deny the access request.

28. (Previously Presented): The method of claim 22 wherein an abstain by any one of the plurality of security plug-ins does not cause the security service to deny the access request.

29. (Previously Presented): The method of claim 22 further comprising:

auditing the determinations of the plurality of access decision mechanisms.

30 – 41. (Canceled)

42. (Currently Amended): The security system of claim 1, wherein computation of a dynamic role occurs immediately before an authorization decision for [[a]] the protected resource.

43. (Currently Amended): The security system of claim 18, wherein computation of a dynamic role occurs immediately before an authorization decision for [[a]] the protected resource.